「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」第二次とりまとめ（案）に対する意見募集の結果について

別紙２

１　概要

これまでの議論の内容をまとめた第二次とりまとめ（案）について、総務省ホームページ及び電子政府の総合窓口を通じ幅広く国民より意見募集を実施。

２　意見募集期間

平成27年7月18日（土）～8月10日（月）

３　意見募集の結果

3者から8件の意見提出

４　意見提出者（計3者）

- 一般社団法人情報処理学会
- ヤフー株式会社
- 日本オラクル株式会社

「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会 第二次とりまとめ（案）」に対して提出された御意見
【意見募集期間：平成 27 年7月 18 日（土）～同8月 10 日（月）】

番号	項目 頁	項目 章	項目 節	該当部分	提出された御意見	御意見に対する考え方	意見提出者
1				とりまとめ（案）全体	サイバー攻撃に関連する、不正な通信への対処や脆弱性な通信装置への対処に関し、相応の検討がなされていると考えますが、現状のままでは根本的な解決は非常に難しい問題です。ひとつの対応策として、免許制度や車検制度の運用をいよいよ真面目に考える時期にきているようにも感じられます。一方で、事故前提という考えに基づき、これら不正な通信や脆弱な通信装置の存在を前提としても、サイバー攻撃の被害に遭わないための対策を検討することも必要と考えます。 検討の観点が通信の秘密の侵害に限定されており、対処策による副作用の可能性やその影響度合い、悪意のある第三者がこれら対策を悪用する余地、などに関する検討が不足していると考えます。例えば、個人情報/プライバシー保護に関しては、事業者が講ずべき「配慮原則」のようなものが示されています。そのような記載があると良いと考えます。モバイル端末や制御機器などインターネット接続形態の多様化、身元を詐称して行われるフィッシング詐欺など IT を使った特殊詐欺の巧妙化などの状況を踏まえると、対策を実施するにあたっては、これらの検討を行い慎重な配慮をもって運用されることを期待いたします。	サイバー攻撃対策の実施にあたっては、攻撃に係る通信に関する情報の取得・利用が必要となる場合があり、通信の秘密について留意することが必要と認識しております。このため、本とりまとめにおいては、通信の秘密等の観点から検討を行いました。なお、本とりまとめ第２章第１節～第４節において、本件対策で取得した通信の秘密に当たる情報を本件対策以外のために利用することは許容されない旨の記載がされております。いただいた御意見は、今後の検討においても参考にさせていただきたいと思います。	一般社団法人情報処理学会
2				とりまとめ（案）全体	研究会における議論及びそのとりまとめ（以下「とりまとめ」といいます。）については、各ＩＳＰがとりまとめに取り上げられたようなサイバー攻撃への対処を行うことが、違法・不当ではないことを担保するものであり、歓迎すべきと考えます。	本とりまとめに対する賛同意見として承ります。	ヤフー株式会社

番号	項目 頁	章	節	該当部分	提出された御意見	御意見に対する考え方	意見提出者
3				とりまとめ（案）全体	この資料で提示されている４つの具体的な項目は、「サイバー攻撃に対する入口・出口対策」について焦点を当て検討を加えたものと想定します。つきましては、以下ように「入口・出口対策に対して検討を加えた」旨の文言の追加を提案します。 ＜提案文＞ 「本報告書は、研究会における議論や検討に基づき、それぞれの課題の解決の方向性、特に、サイバー攻撃に対する入口・出口対策について取りまとめたものである。」 ちなみに、高度化するサイバー攻撃における脅威に対する対策として、入口・出口対策を乗り越えて侵入してくる脅威に対し、データ保護自体も最終防衛ラインとして極めて重要、かつ有効な一手と認識しています。	御指摘の「サイバー攻撃に対する入口・出口対策」が必ずしも明らかではありませんが、本とりまとめP25に記載のとおり、本研究会では、構成員から、優先的に対応すべき課題として挙げられた「C&Cサーバ等との通信の遮断における有効な同意について」等４つの課題を中心に検討を行ったところです。いただいた御意見は、今後の検討においても参考にさせていただきたいと思います。	日本オラクル株式会社
4	p. 12	2	1	(1)	該当部分においては、Ｃ＆Ｃサーバ等と利用者との間における通信の遮断等の対処に係る利用者からの同意の有効性について、記載されています。 しかるに、「（利用者端末と）Ｃ＆Ｃサーバ等との通信は、通信が行われているという事実やその内容について利用者が認知できないままバックグラウンドで実行され（る）」（とりまとめ２頁）状態であることから、たとえ一方通信端末が利用者端末であっても、当然に利用者が一方通信当事者になるとの認定がなされず、攻撃者が一方通信当事者であるとの評価も可能である場合があり得ると思われます。その場合、利用者からの同意の有無は、当該対処に係る違法性阻却事由にはならないことから、違法性阻却に係る法的安定性を高めるため、正当業務行為の観点からも検討が記載されるべきと考えます。	本研究会では、構成員から優先的に対応すべき課題として、C&Cサーバ等との通信の遮断における有効な同意の在り方が検討課題として挙げられました。本とりまとめにおいて、通信が行われているという事実やその内容について利用者が認知できないままバックグラウンドで実行されている C&C サーバ等との通信の遮断に関し、契約約款に基づく事前の包括同意であっても有効な同意といえる場合について整理されたことにより、利用者の有効な同意に基づく行為として、ISPの自社DNSサーバで処理する契約回線からのアクセスに係る FQDN の検知・C&C サーバ等の FQDN の名前解決要求に係る通信の遮断が許容されるものと考えており、この点が明確となるように表現を修正いたします。	ヤフー株式会社

番号	項目			該当部分	提出された御意見	御意見に対する考え方	意見提出者
	頁	章	節				
5	p.14	2	2	(1)(2)	ISP から利用者に対してパスワード変更を依頼する行為について記載されています。このような行為は、ISP を詐称した悪意のある第三者がパスワード変更の依頼し、不正にパスワードを取得することを助長する恐れが考えられます。実施にあたっては、身元詐称が行われる余地の無いよう、適切な手段を講じることが必要と考えます。	本研究会では、他人の ID・パスワードを悪用したインターネットの不正利用への対処について、通信の秘密の観点から検討を行ったところです。御指摘のように、ISP 等において、実際の取組の際には適切な手段を講じることが求められるものと考えております。	一般社団法人情報処理学会
6	p.14	2	2	(2)	ＰＰＰｏＥ認証サーバに係る対処の違法性阻却事由について、取りまとめでは、正当業務行為への該当性の観点から検討が記載されています。しかるに、ＰＰＰｏＥ認証は、利用者（または攻撃者）とＩＳＰとの間の通信であるところ、利用者に係る通信の秘密は他方通信当事者であるＩＳＰに委ねられていることから、当該ＩＳＰがＰＰＰｏＥ認証に関する何らかの対処を行うにあたり、そもそも通信の秘密の侵害に係る論点が惹起されることはないとの見方もあり得ると思われます。したがいまして、この観点からの検討も記載いただくべきと考えます。 ＰＰＰｏＥ認証サーバに係る対処の正当業務行為該当性について、とりまとめでは、認証サーバが異常を検知した「後」を対象とした記載がされているところ、世界中で日々様々な攻撃手法が開発される中で実効性ある対処を継続していくためには、「どのような状態を『異常』と取り扱うか」自体を検討するための研究・分析等も非常に重要であると考えます。しかるに、当該検討のための分析等も、本該当部分の記載によれば目的の正当性・行為の必要性は認められると思われるところ、当該分析等が当代における技術的相当性に照らし相当な範囲であれば、手段の相当性も認められることについても記載いただくべきと考えます。	本とりまとめ P14,15 に記載のとおり、ISP の認証サーバに記録されたタイムスタンプ及び PPPoE 認証の ID は、通信の構成要素として通信の秘密の保護の対象となるため、これらを分析等することは、通信の秘密の窃用等に該当する可能性があると考えられます。 本研究会では、構成員から優先的に対応すべき課題として挙げられたものを中心に検討を行ったところです。いただいた御意見については、これに限らず、技術の進歩や新たな対策などサイバー攻撃を取り巻く環境の変化に応じて、引き続き検討させていただきたいと思います。	ヤフー株式会社

番号	項目			該当部分	提出された御意見	御意見に対する考え方	意見提出者
	頁	章	節				
7	p.16	2	3	(1) (2) (3)	インターネット接続に機能が限定されたブロードバンドルータに対し、信頼のおける通信事業者(ISP)およびその委託先事業者が契約対象の機器に限定し、当該契約者の合意のもとで、通信役務の安定化を阻害する脆弱性に限定した調査を行うのであれば、検討結果の通りであると考えます。しかしながら、これらの制約条件を逸脱した行為が適切に排除されることが担保されない場合、このような調査は非常に危険な行為であると言わざるを得ません。たとえば、公開サーバの脆弱性の調査においては、サーバ管理者と調査実施者の両者間で、実施する時期、調査項目や調査手段など具体的な内容について慎重に事前調整を行います。調査行為が悪用されないよう調査実施時期や調査項目を第三者から秘匿しておきます。調査時においてはサーバの稼働状態を適切に監視し何らかの異常が見られたら速やかに調査を中止するなど、稼働状態に対する調査の影響が最小限となるよう配慮します。このように、脆弱性の調査を行うには十分すぎる配慮がなされるものであり、本件においても、相応の対応が必要と考えます。	本研究会では、脆弱性を有するブロードバンドルータの調査及びその結果を利用した利用者への注意喚起について、不正アクセス禁止法及び通信の秘密の観点から検討を行ったところです。御指摘のように、ISP 等において、実際の取組の際には適切な手段を講じることが求められるものと考えております。	一般社団法人情報処理学会
8	p.25	3		「おわりに」	通信の秘密の侵害について慎重に検討しつつも、有効な同意の範囲や正当業務行為（違法性阻却事由）の範囲を的確に判断し、合理的な結論を得ているものと考えます。また、本件目的以外での取得情報の利用は通信の秘密の侵害にあたる、という明確な整理がなされていることは、これまでの通信の秘密と同意取得および正当業務行為との関係の整理や、消費者にとっての不安感をいたずらに煽ることは避けるべき、という観点からも適切と考えます。ただし、上記の整理について、たとえば第 2 章第 1 節(2)末尾（p.14）や、同章第 3 節(3)末尾（p.22）、同章第 4 節末尾（p.24）などにおいて明記がなされつつも、第 3 章(「おわりに」）や「第二次とりまとめ(案)概要」での言及がないことから、誤った解釈やそれに基づく不安などが流布されてしまう懸念があります。これらの点について誤解などが生じることがないように、概	本とりまとめに対する賛同意見として承ります。 なお、利用目的については、本とりまとめ第２章第１節～第４節においてそれぞれ記載されており、明確になっているものと考えております。	一般社団法人情報処理学会

					要や第 3 章での上記整理の再掲をするなど、より伝わりやすい表現をしていただくことを期待いたします。		